(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－358026
（P2000－358026A）
(43)公開日　平成12年12月26日(2000.12.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ａ
Ｂ４２Ｄ　15/10	５０１	Ｂ４２Ｄ	15/10	５０１Ｌ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ	17/00	Ｖ
				Ｘ
19/07		Ｇ０９Ｃ	1/00	６４０Ｂ

審査請求　有　　請求項の数12　ＯＬ　（全　９　頁）　　最終頁に続く

(21)出願番号　特願2000－110987(P2000－110987)
(62)分割の表示　特願平1－66443の分割
(22)出願日　平成１年３月20日(1989.3.20)

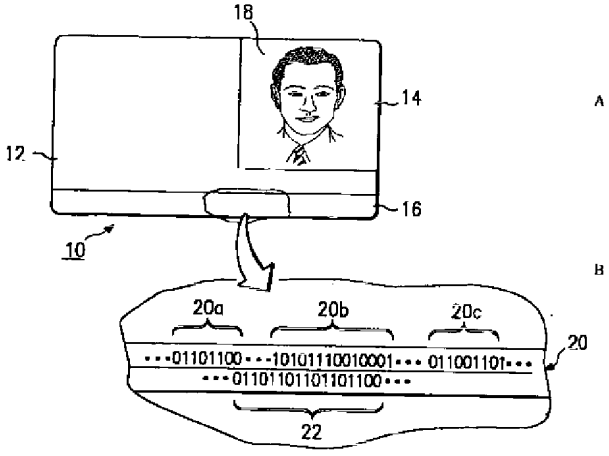
(31)優先権主張番号　０７／１７０７３４
(32)優先日　昭和63年３月21日(1988.3.21)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　500115310
ポラロイド、コーパレイシャン
アメリカ合衆国マサチューシッツ州02139、ケイムブリッジ、テクナラジ・スクウェア　549番
(72)発明者　フランク、ティー、リータン
アメリカ合衆国マサチューシッツ州02160、ニュートンヴィル、チャールスドン・パーク　15番
(74)代理人　100073841
弁理士　真田　雄造　（外２名）

最終頁に続く

(54)【発明の名称】　個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法と個人識別カードをその認可使用者に発行する方法

(57)【要約】　（修正有）
【課題】　認可個人認識カードの認可されない使用を、公開鍵暗号方式を使い防止する。
【解決手段】　公開鍵暗号方式の鍵対の個人用鍵を使用して秘密でないパスワードをディジタル署名に暗号化する。次いでパスワード２０及びディジタル署名を符号化し、カードの磁気条片又は他の記憶デバイスに記憶する。トランザクションを実行するためには、受け取ったカードのディジタル署名を、受け取ったカードのパスワード２０から生成されたものとして示さなければならない。パスワード２０は、トランザクション端末において表示できる認可カード保持者のディジタル写真を含むのが好適である。このことによってトランザクション端末の操作者は、視覚検査によってカード保持者の識別を確認できる。



【特許請求の範囲】

【請求項１】　個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法において、
秘密でない部分を持つパスワードを生成するステップと、
所定の関数Ｆを使い前記パスワードを写像して写像パスワードを生成するステップと、
この写像パスワードを、公開鍵暗号方式の鍵対の個人用鍵でディジタル署名して前記写像パスワードに対応する署名を生成するステップと、
前記パスワード及び署名を符号化して符号化パスワード／署名を生成するステップと、
この符号化パスワード／署名を個人識別カードに記憶するステップと、
この個人識別カードをトランザクション端末において受け取るステップと、
この受け取った個人識別カードの前記符号化パスワード／署名を復号して受信パスワード及び受信署名を生成するステップと、
前記受信パスワードを前記所定関数Ｆで写像して前記受け取った個人識別カードに対する写像パスワードQ_Rを生成するステップと、
前記公開鍵暗号方式の鍵対の公開鍵Ｍを使い、前記受け取った個人識別カードに対する写像パスワードから前記受信署名の所定の関数を生成することができるかどうかのディジタル確認を行うステップと、
この受信署名の所定関数を公開鍵を使い前記写像パスワードから生成することができる場合には、前記受信署名が妥当であるという指示を生成するステップと、
前記受信パスワードから表示を生成するステップと、
前記表示及び指示を前記トランザクション端末のディスプレイに展示して、このトランザクション端末の操作者により使用者が個人識別カードを使いトランザクションを実行するように認可されていることを確認できるようにするステップと、
から成る、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項２】　前記パスワードに、認可使用者の肉体的特性の画像表示を表わすデータを含める請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項３】　前記パスワードに、認可使用者についての１つ又は複数の個人的事項を表わすデータを含める請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項４】　前記パスワードに、それぞれ特定のトランザクションを認可する１つ又は複数のコードワードを含める請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項５】　前記パスワードに、認可使用者の肉体的特性の画像表を表すデータと、前記認可使用者についての１つ又は複数の個人的事項を表わすデータと、前記個人識別カードを使い特定のトランザクションを認可する少なくとも１つのコードワードとを含める請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項６】　所定の関数Ｆとして恒等関数を使う請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項７】　所定の関数ＦとしてＤＥＳ方策に基づくハッシング関数を使う請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項８】　前記符号化パスワード／署名を生成するステップが、前記パスワード及び著名を誤り訂正符号で符号化するステップを含む請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項９】　前記復号して受信パスワード及び受信署名を生成するステップが、符号化パスワード／署名から復号した受信パスワード及び受信署名の誤りを訂正するステップを含む請求項１記載の、個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行できるようにする方法。

【請求項１０】　個人識別カードをその認可使用者に対し発行する方法であって、、
認可使用者の肉体的特性の画像表示を生成するステップと、
この画像表示を処理してパスワードＱを生成するステップと、
このパスワードを所定の一方向関数で写像してこのパスワードの長さより実質的に短い長さを持つ写像パスワードを生成するステップと、
P_1及びP_2が秘密素数であり、第１の公開鍵暗号方式の鍵対が$P_1 \cdot P_2$に等しい公開鍵Ｍを含む場合に、前記写像パスワードＱを前記第１の公開鍵暗号方式の鍵対の個人用鍵（P_1、P_2）でディジタル署名して第１の署名を生成するステップと、
前記パスワード及び第１の署名を誤り訂正符号で符号化して符号化パスワード／署名を生成するステップと、
この符号化パスワード／署名を個人識別カードに記憶するステップと、
から成る、個人識別カードをその認可使用者に対し発行

する方法において、
認可使用者についての１つの又は複数の個人的事項を表わす１つの又は複数の別の個人的データを前記パスワードに沿って記憶するステップをさらに包含する、個人識別カードをその認可使用者に対し発行する方法。
【請求項１１】　個人識別カードを使い特定のトランザクションを認可する１つ又は複数の各コードワードを、前記パスワードにさらに記憶するステップを包含する請求項１０記載の、個人識別カードをその認可使用者に対し発行する方法。
【請求項１２】　それぞれメモリをカード内部に持ち、少なくとも１つのトランザクション端末に使うようにした個人識別カードを初期化する端末において、秘密でない部分を持つパスワードを初期化しようとするカードを持つ使用者に割当てる割当て手段と、割当てられたパスワードの少なくとも一部分からディジタル署名を誘導し各使用者に対するディジタル署名を公開鍵暗号方式の鍵対の個人用鍵により誘導するようにした誘導手段と、誘導された各ディジタル署名を使用者カード内に記憶することを制御する制御手段とを包含する端末。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、一般に個人識別手段、ことに認可個人識別カードを発行しこれ等のカードの非認可の使用をトランザクション処理中に防ぐ方法及びシステムに関する。
【０００２】
【発明の背景】クレジットカード又はその他の個人識別カード用のパスワード使用保護方策は、当業界にはよく知られている。このようなカードは、このカードに固着した磁気テープ又はその他の記憶媒体から成るメモリを備えている。これ等のカードは又、マイクロプロセッサ及び協働する制御プログラムの形のデータ処理機能を持つ。操作時には、カード発行手段により先ずメモリに、個人識別番号すなわち秘密パスワードと共に、最高金額を表わす数値を記憶する。トランザクションを実行するには、カードを端末装置に入れる。この場合ユーザはそのパスワードを入力することが必要である。端末装置が使用者の入力したパスワードとカードに記憶されたパスワードとの間の一致を確認すると、トランザクションを処理することができる。次いでこのトランザクションの数値はカードに残る数値から差引かれ、得られる数値は利用できるユーザ信用額を表わす。
【０００３】従来又、前記したようなクレジットカードの違法な発行に対する防止法が述べられている。ウエインステイン（Ｗｅｉｎｓｔｅｉｎ）を発明者とする米国特許第４，４５３，０７４号明細書では、このような各カードにユーザ秘密パスワード及び共通の基準テキストの連接を暗号化したコードを記憶してある。この暗号化は、公開鍵暗号方式の鍵対の公開鍵に協働する個人用鍵の使用により初期設定すなわち初期化端末内で行われる。操作時にはカード保持者はそのカードをトランザクション端末に差出す。この端末は、公的鍵暗号方式の鍵対の公開鍵により、カードの記憶されたコードを解読する、記憶されたコードがカード保持者のキーボードにより入力したユーザパスワードと共通基準テキストとに解号する場合だけ、トランザクションが実行される。
【０００４】ウエインステインの特許明細書に記載してある方法はクレジットカードの不正の発行を防止する適当な保護手段にはなるが、この手段では各ユーザは、記憶しておいてトランザクション端末に入力しなければならない秘密のすなわち『個人用の』パスワードを持つ必要がある。ウエインステインによれば又、ユーザの秘密パスワードに共通の基準テキストを連接する付加的な回路を必要とする。このような必要により、保護方策の保全を意図的に確実にする必要があると共に、このシステムの複雑さ及び費用が増大する。
【０００５】従ってシステムの秘密を保持するのに、『秘密』パスワードを認可使用者が記憶する必要がなく又は共通の基準テキストに連接する必要のない公開鍵暗号方式を使い個人識別カードを発行する新規な方法を提供することが望ましい。
【０００６】
【発明の簡単な要約】本発明は、認可個人識別カードを発行し、これ等のカードの認可されない使用を公開鍵暗号方式を使い防止する方法及びシステムにある。
【０００７】本発明の１特徴によればカードの認可使用者は、使用者の若干の秘密でないすなわち『公開』特性の表示から生ずる部分を持つパスワードを割当てられる。次いでこのパスワードは処理されディジタル署名を生成する。このディジタル署名は次いで、パスワードと共にカードに記憶される。トランザクション端末でトランザクションを認可するには、受入れたカードからのディジタル署名が先ず受入れカードのパスワードから生成していることを示さなければならない。パスワードは又、トランザクション端末で処理されこのパスワードに符号化された公開『特性』の表示を展示する。次いでこの公開特性は、トランザクションの認可に先立ってトランザクション端末の操作者が確認する。公開鍵がなくてもカードにパスワードに対するサインが真正であるかないかを確認することは簡単であるが、適正な個人用鍵なしで個人データに対し妥当なディジタル署名を生成することは極めてむずかしい。すなわちカード発行手段だけしか妥当なカードを作ることができないし、又一致する個人特性を持つ使用者だけしかカードを使うことができない。
【０００８】好適な実施例ではパスワードは、認可使用者の肉体的特性（たとえば顔、指紋、音声サンプル又は類似物）の画像表示を表わすデータを含む。或は画像表示データのほかにパスワードは、使用者の関係のある他

のデータたとえば使用者の年齢、住所、国籍、セキュリティクリアランス、銀行勘定残高、雇用者、所有権の証明又は類似物を含む。パスワードは又１つ又は複数のコードワードを含む。これ等の各コードワードは、或る日付で或る資金を受ける許可、分類された書類を見る許可、或る日付で或る国に入る許可（すなわち査証）、或る行為を行う認証又は類似事項のような特殊のトランザクションを認可する。限定するわけではないが、個人識別カードは、クレッジットカード、運転者免許証、パスポート、会員カード、年齢証明カード、銀行カード、セキュリティクリアランスカード、法人識別カード又は国籍識別カードがある。

【０００９】好適な実施例では、認可個人識別カードを発行する方法は、認可使用者の肉体的特性の画像表示を生成するステップと、この画像表示を処理してパスワードを生成するステップと、このパスワードを所定の関数で写像して写像されたパスワードを生成するステップと、この写像されたパスワードを公開鍵暗号方式鍵対の個人用鍵によりディジタル署名して写像されたパスワードに対応する署名を生成するステップと、前記パスワード及びサインを所定の関数で符号化して符号化パスワード／署名を生成するステップと、この符号化パスワード／署名を個人識別カードに記憶するステップとから成っている。

【００１０】個人識別カードの認可使用者がトランザクション端末を使いトランザクションを実行することができるように本発明では、個人識別カードをトランザクション端末で受取り、前記受取った個人識別カードの符号化パスワード／署名を復号して受信パスワード及び受信署名を生成し、この受信パスワードを所定の関数で写像して受入れ個人識別カードに対する写像パスワードを生成し、公開鍵暗号方式の鍵対の公開鍵を使い、受け取った個人識別カードに対する写像パスワードから受信署名を生成することができるかどうかのディジタル確認を行うことから成る方法について述べる。公開鍵を使い写像パスワードから受信署名を生成することができれば、本方法は受信署名が妥当であるという指示を生ずることにより継続する。次いで受信パスワードから画像表示を生成し、次いでこの画像表示及び指示をトランザクション端末のディスプレイに展示してその操作者により個人識別カードを使いトランザクションを実行するように使用者が認可されることを確認することができる。

【００１１】本方法のディジタル署名ルーチンは、Ｍ＝$Ｐ_1$・$Ｐ_2$とした場合に４つの因数±１モジュロＭ及び±２モジュロＭの各因数を写像パスワードＱに乗ずるステップを含む。この説明で使う場合にＭは公開鍵暗号方式の鍵対の公開鍵を示し、又（$Ｐ_1$・$Ｐ_2$）はこの公開鍵方式の鍵対の個人用鍵を示す。この場合$Ｐ_1$及び$Ｐ_2$は、４つの値±Ｑ　ｍｏｄ　Ｍと±２Ｑ　ｍｏｄ　Ｍのうち１つの値だけが法Ｍの下で平方剰余になるように前もって選定した秘密素数である。ディジタル署名ルーチンによれば４つの値±Ｑ　ｍｏｄ　Ｍ及び±２Ｑ　ｍｏｄ　Ｍとは、これ等の値のどれが法Ｍの下で平方剰余であるかを定めるように評価する。次いで平方剰余の平方根を計算しディジタル署名を生成する。個人鍵の秘密素数の因数分解を知らないでこの平方根の計算を実施することは極めてむずかしいから、認可されてない第三者はカード『サイン』を生成することができない。このカード『サイン』は、トランザクション端末でディジタル確認を行ったときに受取った個人識別カードの写像パスワードから生成されることを示すことができる。

【００１２】本発明のなお他の特徴によれば、認可個人識別カードを発行し、その認可されない使用を防止するシステムは、それぞれ個人識別カードの１つの発行手段を独特に協働させた複数の発行トランザクション端末を備えている。各発行手段は、システム内の他の各発行手段の公開鍵暗号方式の鍵対とは異なっていてもいなくてもよい各発行手段自体の公開鍵暗号方式の鍵対を割当てられ又は選定する。パスポート管理システム又は類似物にとくに適したこの構造によりトランザクション端末の操作者は１つ又は複数の発行手段からの署名を確認することができる。

【００１３】本発明の別の特徴によれば、少なくとも１つのトランザクション端末を介しトランザクションを実行する独特の個人識別カードが得られる。この識別カードは、本体部分と、この本体部分内に設けられパスワードと、このパスワードから誘導される署名とを記憶するメモリとを備えるのがよい。パスワードは、認可された使用者の秘密でない特性たとえば使用者の顔の画像表示から生成される部分を含んでいる。署名は、公開鍵暗号方式の鍵対の個人用鍵によりパスワードから誘導される。

【００１４】

【実施例】実施例について図面を参照して説明すると本発明の同様な部品又はステップは同様な参照数字を使ってある。図１Ａはトランザクション端末を介しトランザクションを実行するのに、本発明により使用する個人識別カード（１０）を線図的に示す。前記したように本発明によれば『個人識別カード』という用語は、広い意味のもので、クレジットカード又はその他の一般に知られている証明書たとえばパスポート、運転者免許証、会員カード、年齢証明カード、セキュリティクリアランスカード、法人識別カード、国籍証明カード又は類似物を含むものと考えられる。

【００１５】図１Ａの個人識別カード（１０）は運転者免許証である。カード（１０）は、表示（１４）及びメモリ（１６）を持つ本体部分（１２）を備えている。限定するわけではないがメモリ（１６）は、よく知られているようにしてカードに添付した又はその中に埋込んだ磁気条片または類似の媒体、或はＰＲＯＭのような電子

メモリがよい。個人識別カード（１０）は、本体部分に埋込んだ一体のマイクプロセッサを備えていてもいなくてもよい。図１Ａに明らかなように個人識別カード（１０）の表示（１４）は、認可使用者の肉体的特性の画像表示（１８）たとえば使用者の顔を添付してある。表示（１４）は又使用者のその他の肉体的特徴の画像表示たとえば使用者の指紋又は掌紋を展示してもよいのはもちろんである。

【００１６】図１Ｂにおいて本発明によれば個人識別カード（１０）のメモリ（１６）は、使用者の若干の秘密でないすなわち公開特性の表示から生ずる部分（２０ａ）を持ち認可使用者に独特の『パスワード』（２０）を備えるのがよい。この説明で使う『使用でない』という用語は、認可使用者の表示たとえば使用者の顔が個人識別カード及び認可使用者を直接見て比較することにより容易に確かめられるもののことである。好適な実施例ではパスワードの部分（２０ａ）は、個人識別カード（１０）の画像表示（１８）のディジタル化バージョンを表わすディジタルビットストリームである。

【００１７】又図１Ｂに示すようにパスワード（２０）は、認可使用者についての１つ又は複数の個人的事項を表わすデータたとえば使用者の年齢、住所、国籍、セキュリティクリアランス、雇用者、銀行勘定残高、目の色、身長、体重、母親の婚前の姓又はその他任意のこのような情報を持つ部分（２０ｂ）を備えている。この情報は公的のものであってもなくてもよい。さらにパスワード（２０）は、１つ又は複数のコードワードを持つ部分（２０ｃ）を備えている。これ等の各コードワードは、或る日付の入国の許可、或る日付で若干の資金を受ける許可、若干の分類された書類を調査する許可のような特殊なトランザクション、又は１つ又は複数の他のこのような特殊なトランザクション、又は１つ又は複数の他のこのような特殊なトランザクションを認可する。パスワード（２０）は、図１Ｂに示した１種類又は複数種類の所定の形式のデータ部分（２０ａ）、（２０ｂ）又は（２０ｃ）或はこれ等の全部を含んでもよいのはもちろんである。

【００１８】又は図１Ｂに示すように個人識別カード（１０）のメモリ（１６）は署名（２２）を含んでいる。署名（２２）は、なお詳しく後述するように、『公開鍵暗号方式』の鍵対の個人用鍵を使いパスワード（２０）から誘導する。『公開鍵暗号方法式』は、２つの『鍵』を持つ公知の機密保持手段である。一方の鍵は公開のものであり（又は少なくとも鍵対の所有者がこの鍵が公開になるかどうかについて実際上注意を払わない）、又一方の鍵は個人用すなわち非公開のものである。このような公開鍵暗号方式の鍵対はすべて共通の特徴を持つ。すなわち個人用鍵は公開鍵から決定することができない。

【００１９】図２には、図１Ａに示したような認可個人識別カード（１０）を発行する本発明の好適な方法のフローチャートを示してある。ステップ（３０）ではカード発行手段がカード申込者から必要な個人的データを収集する。限定するわけではないがこのデータは、認可使用者の物理的特性の画像表示を含むのがよい。たとえばこのデータはカード申込者の写真を含む。ステップ（３２）では写真、その他の個人的データ又はコードの各認可項目或はこれ等の全部の項目を処理して図１Ｂで述べたようなパスワードを生成する。

【００２０】ステップ（３４）ではこのパスワードを所定の一方向関数Ｆで写像し、パスワードの長さより実質的に短い長さを持つ写像パスワードＱを生成する。この写像ステップは、とくに認可使用者のディジタル化写真を記憶したときに、パスワードを構成するディジタルビットストリームの長さを短縮するのに必要である。単に１例として所定の一方向関数Ｆは、ＤＥＳ方策又はゴールドワッサ、ミカリ及びリベスト（Ｇｏｌｄｗａｓｓｅｒ，Ｍｉｃａｌｉ　＆　Ｒｉｖｅｓｔ）の方策から得られるような複数の公知のハッシング関数（ｈａｓｈｉｎｇ　ｆｕｎｃｔｉｏｎ）のうちの任意の１つ又は複数の関数でよい。或は関数Ｆは、パスワードを修飾を加えないでステップ（３４）を経て単に転送する恒等関数でもよい。この恒等関数は、パスワード長さがメモリ（１６）の利用できる記憶容量より十分に短い場合に使用する。

【００２１】ステップ（３６）では本方法は、引続いて写像パスワードＱを公開鍵暗号方式の鍵対の個人用鍵（P_1・P_2）で『ディジタル署名』を行いいわゆる『署名』を生成する。なお詳しく後述するように好適な実施例ではP_1及びP_2は秘密の基本数字であり、公開鍵暗号方式の鍵対は、P_1・P_2に等しい公開鍵Ｍを含む。ステップ（３８）では本方法は、パスワード（写像パスワードとは異なって）及び署名を誤り訂正符号で符号化して符号化パスワード／署名を生成する。ステップ（３８）では、カード（１０）をそのデータの若干が破壊されても確実に使用可能にする。ステップ（４０）では符号化パスワード／署名は実質的に図１Ｂに示すようにして個人識別カードに記憶される。

【００２２】図２には詳細に示してないが、カード発行手段が互いに異なる公開鍵暗号方式の鍵対のキーを使い互いに異なる１回又は複数回の時間にカード（１０）に１つ又は複数のディジタル署名をディジタルに署名するのは明らかである。この場合このカードは、各署名を異なる国に対応する異なる暗号方式の鍵対から誘導したパスポート（すなわち査証）として機能することができる。又図２の方法では、写像ステップに先だってパスワードを所定の関数で暗号化し又は署名自体を暗号化し或はこれ等の両方を行う付加的な暗号化ステップを含むことが望ましい。このようにしてカードを紛失し又は盗まれても高度に機密を保持することが望ましい情報を付与

することができる。

【００２３】図３には本発明の好適なディジタル署名ルーチンの詳細なフローチャートを示してある。前記したようにＭは公開鍵暗号方式の公開鍵であり、（$Ｐ_1$・$Ｐ_2$）はその個人用鍵である。このルーチンによれば秘密の素数$Ｐ_1$及び$Ｐ_2$はステップ（４２）で、写像パスワードＱに４つの所定の因数±１モジュロＭおよび±２モジュロＭを乗じたときに、得られる値±Ｑ　ｍｏｄ　Ｍ及び±２Ｑ　ｍｏｄ　Ｍのただ１つの値が法Ｍの下で平方剰余になるように選定する。好適なディジタル署名ルーチンの機密保持は主として、Ｍ＝$Ｐ_1$・$Ｐ_2$の因数分解を知らないで法Ｍの下で平方剰余の平方根を計算するのが極めてむずかしいということに基づく。

【００２４】又図３に示すようにステップ（４４）で写像パスワードＱに因数±１　ｍｏｄＭ及び±２　ｍｏｄ　Ｍの各因数を乗ずる。このルーチンはステップ（４６）に続く。ステップ（４６）ではこのようにして得られる各値±Ｑ　ｍｏｄ　Ｍ及び±２Ｑ　ｍｏｄ　Ｍを評価して法Ｍの下で平方剰余を位置指定する。この値を位置指定したときに、ルーチンはこの値の平方根をステップ（４８）で計算してディジタル署名を生成する。

【００２５】詳細には示してないが個人用鍵は任意の数の秘密素数（$Ｐ_1$、$Ｐ_2$、$Ｐ_3$、・・・$Ｐ_n$）を含むのは明らかである。秘密素数は図４に示したルーチンに従って選定するのがよい。ステップ（３５）ではｎ－ビットの乱数Ｘ１を生成する。ビット数ｎは、Ｍを因数に分解にすることがむずかしくなるように十分に大きくする（たとえば２５０ビット）必要がある。ステップ（３７）では$Ｘ_1$を所定の値たとえば３　ｍｏｄ　８に一致するように増分する。ステップ（３９）では$Ｘ_1$が素数であるかどうかを定めるようにテストを行う。$Ｘ_1$が素数であれば、$Ｘ_1$＝$Ｐ_1$をセットすることによりルーチンはステップ（４１）に続く。Ｘ１が素数でなければ、$Ｘ_1$はステップ（４３）で増分され（$Ｘ_1$＝$Ｘ_1$＋８をセットすることにより）、ルーチンはステップ（３９）に戻る。$Ｐ_1$を選定する、ルーチンはステップ（４５）に続き別のｎ－ビット乱数Ｘ２を生成する。ステップ（４７）ではＸ２は第２の所定の値たとえば７　ｍｏｄ　８に一致するように増分する。ステップ（４９）では$Ｘ_2$が素数であるかどうかを定めるようにテストを行う。素数であればルーチンは、$Ｘ_2$＝$Ｐ_2$をセットすることによりステップ（５１）に続く。$Ｘ_2$が素数でなければ、$Ｘ_2$をステップ（５３）で増分し（$Ｘ_2$＝$Ｘ_2$＋８をセットすることにより）、ルーチンはステップ（４９）に戻る。$Ｐ_2$を選定すると公開鍵Ｍをステップ（５５）で$Ｐ_1$・$Ｐ_2$に等しくなるようにセットする。

【００２６】署名を計算するのに応答できる発行端末に$Ｐ_1$及び$Ｐ_2$を記憶することが望ましい。さらに別の公開鍵暗号方式の鍵対（この鍵対では個人用鍵は受信端末にだけしか知られていない）を使うことにより、誰も鍵を見分けることができないで個人用鍵（$Ｐ_1$・$Ｐ_2$）を１つの端末から別の端末に配分することができる。さらに図３のディジタル署名ルーチンが好適であるが、他の方策たとえばＲＳＡ、ゴールドワッサー、ミカリ及びリベストの方策又はレイビン（Ｒｅｂｉｎ）の方策或は、これ等の両方策を使ってもよい。このような方策は又公開鍵の肯定応答を必要とするが、図３のルーチンはこれを必要としない。どの場合にも『署名』を生成する処理は、個人用鍵が分っていれば早いが、さもなければ著しく遅くなる。偽造のカードを発行しようとしても、パスワードを写像パスワードＱ内にハッシュする（ｈａｓｈ）のに一方向関数Ｆの使用によりさらに複雑になる。このようにして、偽造者がどうにかしてにせの個人データに対する署名を得られたとしても、偽造者はカード生成方策に選定テキストのアタックを加えることが実際上できなくなる。

【００２７】図５には、図２ないし図３のルーチンに従って発行された個人識別カード（１０）の認可されない使用を防止する好適な方法のフローチャートを示してある。ステップ（５０）では個人識別カードをトランザクション端末において受け取る。ステップ（５２）では符号化パスワード／署名を復号して受信パスワード及び受信署名を生成する。本方法は、受信パスワード及び受信署名の誤りをよく知られた方法に従って訂正するステップ（５４）を含むのがよい。ステップ（５６）では、発行端末で使う同じ所定の関数Ｆで受信パスワードを写像して受入れ個人識別カードに対する写像パスワードＱＲを生成する。

【００２８】次いでこのルーチンはステップ（５８）に続き受信署名が『妥当』であることを確認する。とくに本方法では、公開鍵暗号方式の鍵対の公開鍵を使い、受信署名を写像パスワード$Ｑ_R$から生成することができるかどうかのディジタル確認を行う。生成できるならば本方法はステップ（６０）に続き受信署名が妥当であるという指示を生ずる。ステップ（６２）では、受信パスワードのデータから表示を生成する。この表示は、カードに記憶されたもとのパスワードが認可カード保持者のディジタル化された写真を含んでいれば画像である。ステップ（６２）は署名の確認が行われている間に画像をすぐに展示できるようにステップ（５８）、（６０）と並列に実施することができるのはもちろんである。図５に示すようにステップ（６４）では本方法はトランザクション端末のディスプレイに画像表示又は指示或はその両方を展示する。次いでこのディスプレイは端末の操作者がステップ（６６）で確認してカード保持者が認可されトランザクションを確実に実行する。

【００２９】図２の方法により生成した個人識別カードが使用者識別を必要とするいずれの場合にも使用できるのは明らかである。限定するわけではないがたとえば認可使用者は、購入品の支払いのために認可販売員にカー

ドを差出す。販売員は、このカードをトランザクション端末に入れる。この端末は、カードのメモリからデータを読出し、このカードのディジタル署名が妥当であることを確認し、パスワードから誘導される情報をディスクプレイスクリーンに展示することができる。従って販売員は、カード保持者の身元が主張通りであることを確認し勘定を処置することができる。

【００３０】図６には、図３の好適なディジタル確認ルーチンの詳細なフローチャートを示してある。ステップ（６８）ではルーチンは、受入れ個人識別カードからの写像パスワードQ_Rに因数値±１　ｍｏｄ　Ｍ及び±２　ｍｏｄ　Ｍの各因数を乗ずる。本方法は、受信署名を、Ｍを法として平方することによりステップ（７０）に続き値Ｘを生ずる。ステップ（７２）ではＸが±Ｑｍｏｄ　Ｍ又は±２Ｑｍｏｄ　Ｍのいずれかに等しいかどうかを定めるようにテストを行う。等しい場合にはルーチンはステップ（７４）に続き、受信署名が妥当であるという指示を生ずる。Ｘがこれ等の４つの因数のいずれにも等しくない場合には、署名は不当であり、トランザクションは抑止される。

【００３１】本発明の方法及びシステムは、複数の団体が互いに異なる暗号方式の鍵対を使いカードを発行しようとするが、確認者（すなわちトランザクション端末の操作者）はどの発行手段からのカードも認証することを必要とする多重発行手段シナリオに容易に適合するのはもちろんである。このことは、各発行手段に使われる公開鍵を各トランザクション端末に符号化して入れ、次いでその操作者がこの端末にカード自体と共に発行手段の一致性を端末に入れることによって行われる。或はカード発行手段の一致性をカードに符号化してもよい。このようなシステムは図７に示してある。

【００３２】図７では認可個人識別カードの１つ又は複数の独立の発行手段に対し複数の発行端末（７６ａ）、・・・（７６ｎ）を設けてある。独立の各発行手段は、他の発行手段には知られていない独特の公開鍵暗号方式を割当てられ又は選択する。前記したようにこのような各鍵対の公開鍵は、全部の発行手段に共用の１つ又は複数の各トランザクション端末（７８ａ）、・・・（７８ｎ）に符号化して入れられる。

【００３３】図７のシステムは、パスポート管理、国籍証明カード又は多重会社クレジットカードに対し有用であるが、このような用途に限るものではない。パスポートシステムの操作に当たっては各国は、その発行する個人識別カードに対し完全な自律性を持つ。しかしいずれの国の署名（査証を含む）も認証するのに単一のトランザクション端末が使われる。

【００３４】本発明の方法及びシステムが既存のハードウエア及びソフトウエアで容易に実施できることは、詳細には述べないが当業者には明らかである。好適な実施例では図７に示すように各発行端末（７６）は、図２の方法の各ステップを実施するように、マイクロコンピュータ（８０）とオペレーティングプログラム及び応用プログラムを記憶する協働するメモリデバイス（８２）とを備えている。キーボード（８４）及びディスプレイ（８６）のような入力デバイス及び出力デバイスは、端末及びカード発行手段に対するインタフェースとして設けてある。前記方法の各ステップのうちの１つ又は複数（たとえばディジタル署名ステップ、写像ステップ及び符号化ステップ）がゲートアレイ論理チップ又はソフトウエアで実施できるのはもちろんである。なお各トランザクション端末（７８）も、マイクロプロセッサ（８８）、協働するメモリ（９０）及び適当な入出力デバイスたとえばカード読取り機（９２）、キーボード（９４）及びディスプレイ（９６）を備えるのがよい。

【００３５】前記の説明はとくに個人識別カード用の保護手段に関連するが、本発明のパスワード／署名機密保持ルーチンが又、個人データを識別カード自体に記憶するのでなくて通信チャネルで伝送する場合にも使用できるのは明らかである。又図７に示した本発明の構造は、発行端末（７６ｂ）及びトランザクション端末（７８ａ）の間に通信チャンネル（１００）たとえばモデムを介する電話回線を設けることによって得られる。

【００３６】操作に当たっては図２の各方法ステップは、ステップ（４０）を除きその代りに通信チャネル（１００）により符号化パスワード／署名を伝送するステップを設けることを除いて前記したのと同じである。又図５の確認ルーチンのステップ（５０）を除き代りに、通信チャネル（１００）により得られる情報をトランザクション端末に受け取るようにするステップを設け、次いで図５のステップの残りに従って処理するようにしてもよい。このようにしてパスワード及び署名を含んで伝送する媒体が識別カードでなくて通信チャネル自体である場合に、個人識別に対しパスワード／署名方法が使われる。

【００３７】以上本発明をその実施例について詳細に説明したが本発明はなおその精神を逸脱しないで種種の変化変型を行うことができるのはもちろんである。

【図面の簡単な説明】

【図１】Ａは認可された識別カード使用者の肉体的特性の画像を持つ本発明個人識別カードの１実施例の線図的平面図である。ＢはＡの識別カードの画像から一部を生成したパスワードを示すこのカードの磁気条片の部分の線図的平面図である。

【図２】図１のような認可個人識別カードを発行する本発明の好適な方法のフローチャートである。

【図３】図２のディジタル署名ルーチンの詳細なフローチャートである。

【図４】個人用鍵（P_1・P_2）の秘密素数を選定するルーチンのフローチャートである。

【図５】図３の方法により発行された図１Ａの個人識別

カードの認可されない使用を防止する本発明の好適な方法のフローチャートである。

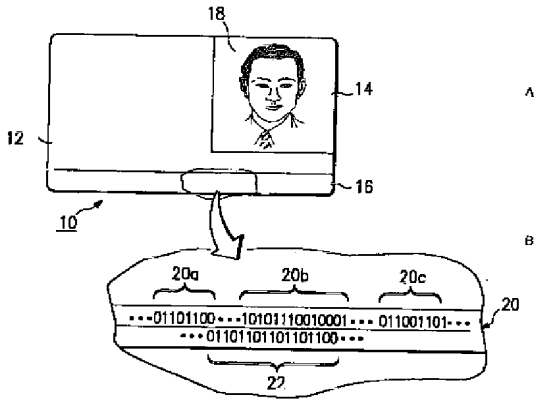
【図６】図５のディジタル確認ルーチンの詳細のフローチャートである。

【図７】本発明による多重発行システムの１例のブロック図である。

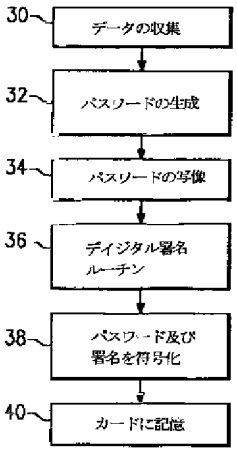
【符号の説明】

１０　個人識別カード
１２　本体部分
１６　メモリ
２０　パスワード
２２　署名
７６　発行端末
７８　トランザクション端末
８０　マイクロプロセッサ
８２　メモリデバイス
８６　ディスプレイ
８８　マイクロプロセッサ
９０　メモリ
９２　カード読取り機
９６　ディスプレイ
１００　通信チャネル

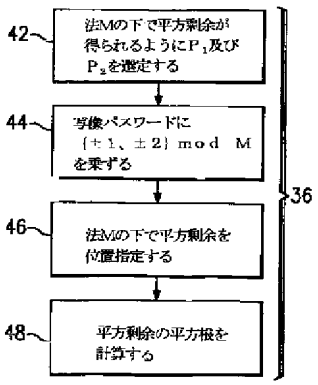
【図１】



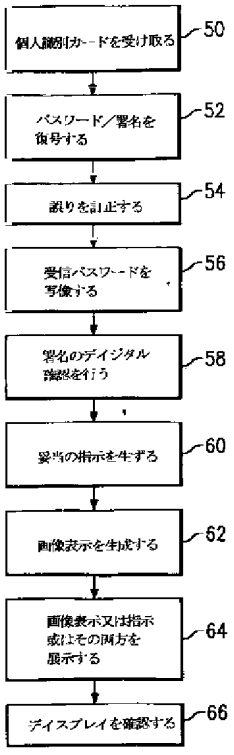
【図２】



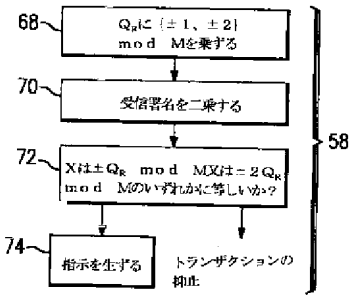
【図３】



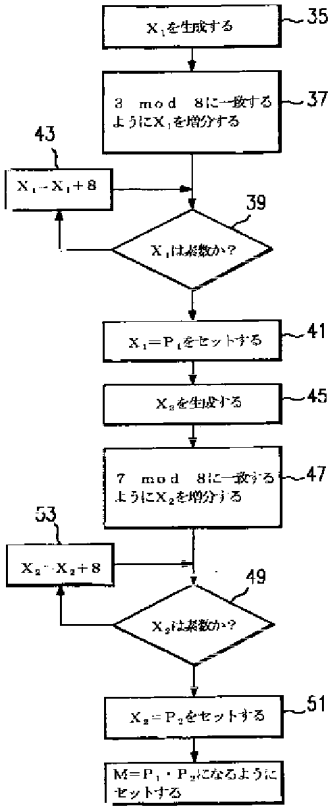
【図５】



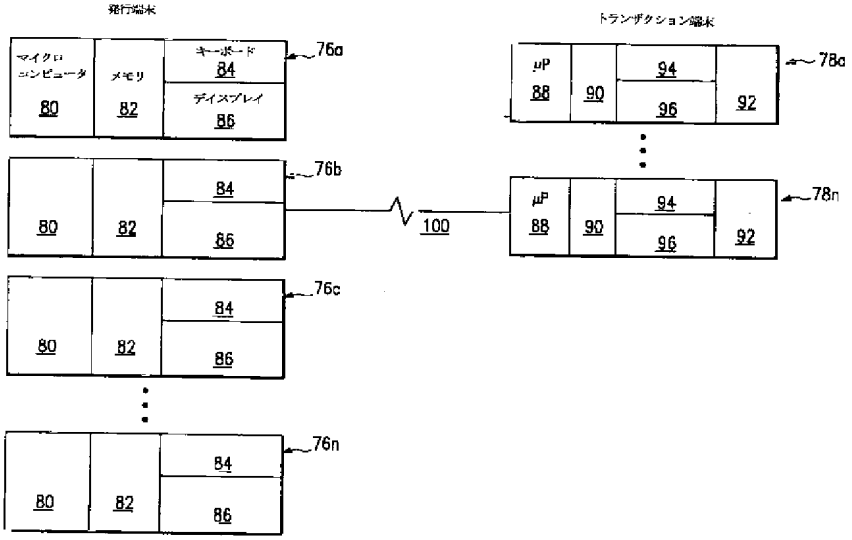
【図６】



【図4】



【図7】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
G06K 19/10		G06K 19/00	J
G09C 1/00	640		S
		H04L 9/00	673E
			673D

(72)発明者 シルヴィオ、ミカーリ
アメリカ合衆国マサチューシッツ州02146
ブルックライン、チェスナット・ヒル・アヴィニュー 459番